UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	35.C14352
First Named Inventor or Application Identifier	
MASAHIKO YAMAGUCHI	
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. ☒ Specification *Total Pages* 23

3. ☒ Drawing(s) *(35 USC 113)* *Total Sheets* 12

4. ☒ Oath or Declaration *Total Pages* 1

a. □ Newly executed (original or copy)

b. ☒ Unexecuted for information purposes

c. □ Copy from a prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 17 completed)
[Note Box 5 below]

i □ DELETION OF INVENTOR(S)
Signed Statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. □ Incorporation By Reference *(useable if Box 4c is checked)*
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4c, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. □ Microfiche Computer Program *(Appendix)*

7. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)

a. □ Computer Readable Copy

b. □ Paper Copy (identical to computer copy)

c. □ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. □ Assignment Papers (cover sheet & document(s))

9. □ 37 CFR 3.73(b) Statement *(when there is an assignee)* □ Power of Attorney

10. □ English Translation Document *(if applicable)*

11. □ Information Disclosure Statement (IDS)/PTO-1449 □ Copies of IDS Citations

12. □ Preliminary Amendment

13. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)

14. □ Small Entity Statement(s) □ Statement filed in prior application Status still proper and desired

15. □ Certified Copy of Priority Document(s)
(if foreign priority is claimed)

16. □ Other:____________________

17. If a CONTINUING APPLICATION, *check appropriate box and supply the requisite information:*

□ Continuation □ Divisional □ Continuation-in-part (CIP) of prior application No. ________

18. CORRESPONDENCE ADDRESS

☒ Customer Number or Bar Code Label 05514 (Insert Customer No. or Attach bar code label here) or □ Correspondence address below

NAME					
Address					
City		State		Zip Code	
Country		Telephone		Fax	

CLAIMS	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
	TOTAL CLAIMS (37 CFR 1.16(c))	18-20 =	0	X $ 18 00 =	$ 0.00
	INDEPENDENT CLAIMS (37 cfr 1.16(b))	6-3 =	3	X $ 78.00 =	$ 234.00
	MULTIPLE DEPENDENT CLAIMS (if applicable) (37 CFR 1.16(d))			$ 260.00 =	$ 0.00
				BASIC FEE (37 CFR 1.16(a))	$ 690.00
			Total of above Calculations =		$ 924.00
	Reduction by 50% for filing by small entity (Note 37 CFR 1.9, 1.27, 1 28).				
				TOTAL =	$ 924.00

19. Small entity status

a. □ A Small entity statement is enclosed

b. □ A small entity statement was filed in the prior nonprovisional application and such status is still proper and desired

c □ Is no longer claimed.

20. ☒ A check in the amount of $924.00 to cover the filing fee is enclosed.

21. □ A check in the amount of $_______ to cover the recordal fee is enclosed.

22. The Commissioner is hereby authorized to credit overpayments or charge the following fees to Deposit Account No` 06-1205:

a. ☒ Fees required under 37 CFR 1 16.

b. □ Fees required under 37 CFR 1.17.

c. □ Fees required under 37 CFR 1.18

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED	
NAME	Brian L. Klock - Reg. No. 36,570
SIGNATURE	
DATE	March 17, 2000

BLK\cmv

DATA PROCESSING APPARATUS AND METHOD FOR ENCRYPTION OR DECRYPTION OF COMMUNICATION DATA

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a data processing apparatus and method for encryption or decryption of communication data.

Related Background Art

It is necessary for an information apparatus connected to a network to prevent data sniffing and wiretapping by third parties. In order to prevent such illegal acts, data ciphering is very effective.

As a cryptosystem becomes more complicated, it takes a longer time to perform a cipher process. For example, in transmitting print data encrypted at a personal computer via a network and printing decrypted data with a printer, the total printing speed is lowered because of encryption and decryption processes.

SUMMARY OF THE INVENTION

It is an object of the invention to solve the above problem and provide a data processing apparatus and method capable of shortening a time required for encryption and decryption while the data security is retained.

According to one aspect, the present invention which achieves these objectives relates to a data processing apparatus comprising: input means for inputting data to be transmitted; extracting means for extracting a particular portion of the data input from the input means; encrypting means for encrypting the particular portion extracted by the extracting means; and transmitting means for transmitting the particular portion encrypted by said encrypting means and a remaining portion not extracted by the extracting means.

According to another aspect, the present invention which achieves these objectives relates to a data processing apparatus comprising: receiving means for receiving data; extracting means for extracting an encrypted portion from data received by the receiving means; analyzing means for analyzing the extracted portion extracted by the extracting means; and output means for outputting the portion analyzed by the analyzing means and a remaining portion not extracted by the extracting means.

According to still another aspect, the present invention which achieves these objectives relates to a data processing method comprising: an input step of inputting data to be transmitted; an extracting step of extracting a particular portion of the data input at the input step; an encrypting step of encrypting the particular portion extracted at the extracting step:

and a transmitting step of transmitting the particular portion encrypted at the encrypting step and a remaining portion not extracted at the extracting step.

According to yet another aspect, the present invention which achieves these objectives relates to a data processing method comprising: a receiving step of receiving data; an extracting step of extracting an encrypted portion from data received at the receiving step; an analyzing step of analyzing the extracted portion extracted at the extracting step; and an output step of outputting the portion analyzed at the analyzing step and a remaining portion not extracted at the extracting step.

According to another aspect, the present invention which achieves these objectives relates to a computer readable storage medium storing a data processing program for controlling a computer to perform data processing, said program comprising codes for causing the computer to perform: an input step of inputting data to be transmitted; an extracting step of extracting a particular portion of the data input at the input step; an encrypting step of encrypting the particular portion extracted at the extracting step: and a transmitting step of transmitting the particular portion encrypted at the encrypting step and a remaining portion not extracted at the extracting step.

According to another aspect, the present invention which achieves these objectives relates to a computer readable storage medium storing a data processing program for controlling a computer to perform data processing, said program comprising codes for causing the computer to perform: a receiving step of receiving data; an extracting step of extracting an encrypted portion from data received at the receiving step; an analyzing step of analyzing the extracted portion extracted at the extracting step; and an output step of outputting the portion analyzed at the analyzing step and a remaining portion not extracted at the extracting step.

Other objectives and advantages besides those discussed above shall be apparent to those skilled in the art from the description of preferred embodiments of the invention which follows. In the description, reference is made to accompanying drawings, which form a part of the invention, and which illustrates an example of the invention. Such example, however, is not exhaustive of the various embodiments of the invention, and therefore reference is made to the claims which follow the description for determining the scope of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating a first embodiment of the invention.

Fig. 2 is a block diagram illustrating the first embodiment of the invention.

Fig. 3 is a flow chart illustrating an example of the operation on an encryption side.

Fig. 4 is a flow chart illustrating an example of the operation on a decryption side.

Fig. 5 is a block diagram illustrating a second embodiment of the invention.

Fig. 6 is a diagram illustrating the structure of image data according to the second embodiment of the invention.

Fig. 7 is a flow chart illustrating an example of the operation according to the second embodiment of the invention.

Fig. 8 is a block diagram illustrating a third embodiment of the invention.

Figs. 9A, 9B and 9C illustrate the structure of voice data according to the third embodiment of the invention.

Fig. 10 is a flow chart illustrating an example of the operation according to the third embodiment of the invention.

Fig. 11 is a block diagram illustrating a fourth embodiment of the invention.

Fig. 12 is a flow chart illustrating an example of the operation according to the fourth embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

<First Embodiment>

Figs. 1 and 3 illustrate the first embodiment of the invention. In this embodiment, encryption of print data to be transmitted from a printer will be described. In this example, of print data, only control codes which determine the fundamental operation of a printer are encrypted. The control codes are important codes which determine the analysis method of data which follows the preceding control code. If the control codes are encrypted, the analysis method for following data can be kept in secret, and sufficient cipher security can be expected even if all print data is not encrypted.

With reference to Fig. 1, the structure of an encryption apparatus will be described. In Fig. 1, reference numeral 1 represents a print data input part for inputting print data. Reference numeral 2 represents an input buffer for tentatively storing print data. Reference numeral 3 represents a data analysis/extracting part for analyzing the contents of print data stored in the input buffer 2 and extracting control codes to be encrypted. Reference numeral 4 represents an encrypting part for encrypting the control codes extracted by the data analysis/extracting part 3. Reference numeral 5 represents an output buffer for tentatively storing encrypted data and remaining data not encrypted, as the data to be transmitted. Reference numeral 6 represents a transmitting part for transmitting data in the output buffer 5.

With reference to Fig. 2, the structure on a decryption side will be described. In Fig. 2, reference numeral 21 represents a receiving part for receiving encrypted communication data. Reference numeral 22 represents an input buffer for tentatively storing received data to be decrypted. Reference numeral 23 represents an extracting part for discriminating and extracting encrypted data in the data stored in the input buffer 22. Reference numeral 24 represents a decrypting part for decrypting the data extracted by the extracting part 23. Reference numeral 25 represents an output buffer for tentatively storing data to be printed. Reference numeral 26 represents an output part for outputting data stored in the output buffer 25.

Fig. 3 is a flow chart illustrating an example of the operation to be executed on the encryption side. Print data input from the print data input part 1 is tentatively stored in the input buffer (S301), and the contents of the data are analyzed by the data analysis/extracting part 3 by a discrimination method such as pattern matching (S302). In accordance with the data analysis result, it is checked whether or not the data is the printer control code (S303). A part of the data recognized as the printer control code by the data analysis/extracting part 3 is encrypted by the encrypting part 4 (S304) and sent to the output buffer 5 (S305). Data except the printer control code is not subjected to the encryption process but is directly sent to the output buffer 5 in which it is synthesized with the encrypted control codes (S306). Thereafter, the contents in the output buffer 5 are transmitted from the transmitting part 6 (S307).

Fig. 4 is a flow chart illustrating an example of the operation on the decryption side. Encrypted data and not encrypted data received by the receiving part 21 are tentatively stored in the input buffer 22 (S401), the contents of the encrypted data in the input buffer 22 are analyzed (S402), and in accordance with the data analysis result, the extracting part 23 discriminates between the encrypted data and the data not encrypted (S403). The encrypted data is extracted by the extracting part 23, decrypted by the decrypting part 24 by a decrypting process (S404) and output to the output buffer (S405). The data not encrypted is directly sent to the output buffer 25 in which it is synthesized with the decrypted control codes without performing decrypting process (S406). Thereafter, the contents in the output buffer 25 are output from the output part 26 to a printer or the like which analyzes the print codes and prints the print data.

In this embodiment, not all the communication data is encrypted, but only the important portion thereof is encrypted. It is therefore possible to shorten the time required for ciphering communication data.

<Second Embodiment>

Fig. 5 illustrates the second embodiment of the invention. In this example, image data is encrypted. Only those image data having a high weight portion of image information representation is encrypted. It is assumed that each pixel of image data is represented by R, G and B primary three colors each having eight bits, totalling in 24 bits per pixel.

In Fig. 5, reference numeral 61 represents an image data input part for inputting image data. Reference numeral 62 represents an input buffer for tentatively storing image data. Reference numeral 63 represents a data extracting part for extracting upper four bits of each R, G and B data stored in the input buffer 62. Reference numeral 64 represents an encrypting part for encrypting the data extracted by the data extracting part 63. Reference numeral 65 represents an output buffer for tentatively storing data to be transmitted. Reference numeral 66 represents a transmitting part for transmitting data in the output buffer 65.

Next, the structure of image data will be described with reference to Fig. 6. As described above, each pixel of image data is represented by R, G and B primary three colors each having eight bits, totalling in 24 bits per pixel. Image data having a high weight portion of image information representation is upper bits. For example, if the upper four bits of eight bits of each R, G and B data are lost, it is almost impossible to recover the original correct image data. Therefore, if the upper four bits only are encrypted, the distinctive ciphering effects can be expected even if all the image data is not encrypted.

Fig. 7 is a flow chart illustrating an example of the operation according to this embodiment. Image data input from the image data input part 61 is tentatively stored in the input buffer 62 (S701), and thereafter analyzed by the extracting part 63 (S702). Only the upper four bits of each of R, G and B three colors are extracted by the extracting part (S703), the upper four bits are encrypted by the encrypting part 64 (S704) and sent to the output buffer 65 (S705). The remaining data of lower four bits is not encrypted, but is directly sent to the output buffer 65 (S706). Thereafter, the contents in the output buffer 65 are transmitted from the transmitting part 66 (S707).

<Third Embodiment>

Fig. 8 illustrates the third embodiment of the invention. In this embodiment, voice data is encrypted. It is assumed that the voice data is constituted of each sampling data of 16 bits subjected to pulse code modulation (PCM).

In Fig. 8, reference numeral 91 represents a voice data input part for inputting voice data. Reference numeral 92 represents an input buffer for tentatively storing voice data. Reference numeral 93 represents an extracting part for extracting four bits including 15th, 11th, 7th and 3rd bits from the data stored in the input buffer 92. Reference numeral 94 represents an encrypting part for encrypting the data extracted by the extracting part 93. Reference numeral 95 represents an output buffer for tentatively storing data to be transmitted. Reference numeral 96 represents a transmitting part for transmitting data in the output buffer 95.

With reference to Figs. 9A to 9C, the structure of voice data will be described. Voice data is constituted of each sampling data of 16 bits subjected to PCM as shown in Fig. 9C. Voice data having a high weight portion of voice information representation is upper bits. Therefore, if the upper bits only are encrypted, it is almost impossible to recover original correct voice information. However, voice data having a low record level has a high possibility that the upper bits thereof are not used and they may become 0. If the third party taps this voice data and the encrypted unknown bits are masked to 0, the voice data at the low record level can be easily recovered. In order to avoid this, in this embodiment, for example, a voice waveform such as shown in Fig. 9A is encrypted by extracting discrete four bits including 15th, 11th, 7th and 3rd bits from all 16 bits.

Fig. 10 is a flow chart illustrating an example of the operation according to this embodiment. Voice data input form the input part 91 is tentatively stored in the input buffer 92 (S1001). Thereafter, the extracting part 93 analyzes the data (S1002), extracts four bits including 15th, 11th, 7th and 3rd bits (S1003), and the encrypting part 94 encrypts the four bits (S1004) and sends the encrypted bits to the output buffer 95 (S1005). The remaining 12-bit data is not encrypted but is directly sent to the output buffer 95 (S1006). Thereafter, the contents of the output buffer 95 are transmitted from the transmitting part 96 (S1007).

<Fourth Embodiment>

Fig. 11 illustrates the fourth embodiment of the invention. In this embodiment, compressed data is encrypted. One of widely used data compression methods is to form a conversion table using Huffman codes assigned a smaller number of bits in the order from a pattern having a higher use frequency and to execute data conversion/compression by using this table. When compressed data is to be expanded, the same conversion table is used. In this embodiment, data is compressed and only the data corresponding to the conversion table is encrypted to make it difficult to recover the original data from the tapped data, thus realizing the effects equivalent to those when all the data is encrypted.

In Fig. 11, reference numeral 111 represents a data input part for inputting data. Reference numeral 112 represents an input buffer for tentatively storing input data input by data input part 111. Reference numeral 113 represents a data distribution analyzing part for analyzing the distribution of patterns used in the data stored in the input buffer 112. Reference numeral 114 represents a conversion table generating part for generating a compression conversion table in accordance with the analysis result of the data distribution analyzing part 113. Reference numeral 115 represents a data conversion compressing part for compressing input data by using the conversion table generated by the conversion table generating part 114. Reference numeral 116 represents a conversion table encrypting part for encrypting the conversion table generated by the conversion table generating part 114. Reference numeral 117 represents an output buffer for storing the compressed data generated by the data conversion compressing part 115 and the table generated by the conversion table encrypting part 116. Reference numeral 118 represents a transmitting part for transmitting the contents in the output buffer 117.

Fig. 12 is a flow chart illustrating an example of the operation according to this embodiment. Data input form the input part 111 is tentatively stored in the input buffer 112 (S1201). Thereafter, the distribution of patterns in the data is analyzed by the data analyzing part 113 (S1202). In accordance with the analysis result, the compression conversion table is generated by the conversion table generating part (S1203). This conversion table is encrypted by the conversion table encrypting part 116 (S1204) and sent to the output buffer 117 (S1205). The data conversion compressing part 115 compresses the input data by using the conversion table (S1206), and the compressed data is directly supplied to the output buffer 117 without being encrypted (S1207). After all data in the output buffer 117 is processed completely (S1208), the contents of the output buffer 117 are transmitted from the transmitting part 118 (S1209).

As described above, according to the embodiments, all the communication data is not encrypted but only the important data among the communication data is encrypted to shorten the time required for the total cipher process.

The invention is applicable not only to

communications between different user terminals but also to communications between a data processing apparatus such as a computer and a storage device such as a hard disk, i.e., to data read/write.

The invention is applicable to a system constituted of a plurality of apparatuses (e.g., a computer, interface units, a display and the like) or to a single apparatus, so long as the functions of each of the embodiments can be realized.

The scope of the invention includes the case wherein a system or apparatus connected to various devices which realize the functions of each of the embodiments, is supplied with software program codes realizing the functions of each embodiment and a computer (CPU or MPU) of the system or apparatus reads and executes the programs code to operate the devices. In this case, the program codes themselves stored in a storage medium realize the functions of each embodiment. Therefore, means for supplying the program codes to the computer, e.g., a storage medium storing such program codes, constitutes the present invention.

The storage medium for storing such program codes may be a floppy disk, a hard disk, an optical disk, a magnetooptical disk, a CD-ROM, a CD-R, a magnetic tape, a nonvolatile memory card, a ROM or the like.

It is obvious that the scope of the invention also contains not only the case wherein the functions of each embodiment can be realized by executing the program codes read by a computer, but also the case wherein the functions of each embodiment can be realized by an operating system (OS) running on the computer or by other application software, in accordance with the program codes.

It is obvious that the scope of the invention also contains the case wherein the functions of each embodiment can be realized by writing the program codes read from the storage medium into a memory of a function expansion board inserted into a computer or of a function expansion unit connected to the computer, and thereafter by executing a portion or the whole of actual processes by a CPU or the like of the function expansion board or function expansion unit.

If the invention is to be applied to the storage medium, this storage medium stores therein program codes corresponding to the operation described with each of the flow charts described above.

Although the present invention has been described in its preferred form with a certain degree of particularity, many apparently widely different embodiments of the invention can be made without departing from the spirit and the scope thereof. It is to be understood that the invention is not limited to the specific embodiments thereof except as defined in the appended claims.

WHAT IS CLAIMED IS:

1. A data processing apparatus comprising:

input means for inputting data to be transmitted;

extracting means for extracting a particular portion of the data input from the input means;

encrypting means for encrypting the particular portion extracted by the extracting means; and

transmitting means for transmitting the particular portion encrypted by said encrypting means and a remaining portion not extracted by the extracting means.

2. A data processing apparatus according to claim 1, wherein the data is print data, and the extracting means extracts a print control code from the print data as the particular portion.

3. A data processing apparatus according to claim 1, wherein the data is image data whose one pixel has a plurality of bits, and the extracting means extracts predetermined upper bits of each pixel from the image data as the particular portion.

4. A data processing apparatus according to claim 1, wherein the data is voice data encoded into codes each having a plurality of bits, and the extracting means extracts predetermined discrete bits of each code

from the encoded voice data as the particular portion.

5. A data processing apparatus according to claim 4, wherein the extracting means extracts bits at a predetermined interval of bits from each code.

6. A data processing apparatus according to claim 1, wherein the data is data compressed by using a conversion table, and the extracting means extracts the conversion table from the compressed data as the particular portion.

7. A data processing apparatus according to claim 1, wherein the transmitting means comprises:

transmission buffer means;

synthesizing means for synthesizing the particular portion encrypted by the encrypting means and the remaining portion not extracted by the extracting means, on the transmission buffer means; and

transmission control means for controlling to transmit data synthesized by the synthesizing means.

8. A data processing apparatus comprising:

receiving means for receiving data;

extracting means for extracting an encrypted portion from data received by the receiving means;

analyzing means for analyzing the extracted portion extracted by the extracting means; and

output means for outputting the portion analyzed by the analyzing means and a remaining portion not extracted by the extracting means.

9. A data processing apparatus according to claim 8, wherein the data is print data, and the encrypted portion is a print control code.

10. A data processing apparatus according to claim 8, wherein the data is image data whose one pixel has a plurality of bits, and the encrypted portion is predetermined upper bits of each pixel of the image data.

11. A data processing apparatus according to claim 8, wherein the data is voice data encoded into codes each having a plurality of bits, and the encrypted portion is predetermined discrete bits of each code.

12. A data processing apparatus according to claim 11, wherein the encrypted portion is bits of each code at a predetermined interval of bits.

13. A data processing apparatus according to claim 8, wherein the data is data compressed by using a

conversion table, and the encrypted portion is the conversion table.

14. A data processing apparatus according to claim 8, wherein the output means comprises:

output buffer means;

synthesizing means for synthesizing the particular portion encrypted by the encrypting means and the remaining portion not extracted by the extracting means, on the output buffer means; and

output control means for controlling to transmit data synthesized by the synthesizing means.

15. A data processing method comprising:

an input step of inputting data to be transmitted;

an extracting step of extracting a particular portion of the data input at the input step;

an encrypting step of encrypting the particular portion extracted at the extracting step: and

a transmitting step of transmitting the particular portion encrypted at the encrypting step and a remaining portion not extracted at the extracting step.

16. A data processing method comprising:

a receiving step of receiving data;

an extracting step of extracting an .encrypted portion from data received at the receiving step;

an analyzing step of analyzing the extracted portion extracted at the extracting step; and

an output step of outputting the portion analyzed at the analyzing step and a remaining portion not extracted at the extracting step.

17. A computer readable storage medium storing a data processing program for controlling a computer to perform data processing, said program comprising codes for causing the computer to perform:

an input step of inputting data to be transmitted;

an extracting step of extracting a particular portion of the data input at the input step;

an encrypting step of encrypting the particular portion extracted at the extracting step: and

a transmitting step of transmitting the particular portion encrypted at the encrypting step and a remaining portion not extracted at the extracting step.

18. A computer readable storage medium storing a data processing program for controlling a computer to perform data processing, said program comprising codes for causing the computer to perform:

a receiving step of receiving data;

an extracting step of extracting an encrypted portion from data received at the receiving step;

an analyzing step of analyzing the extracted portion extracted at the extracting step; and

an output step of outputting the portion analyzed at the analyzing step and a remaining portion not extracted at the extracting step.

ABSTRACT OF THE DISCLOSURE

In order to shorten the time required for encryption and decryption of communication data, the contents of input data are analyzed by a discrimination method such as pattern matching, and in accordance with this analysis result, it is checked whether the received data is particular data. A portion of data judged as the particular data is encrypted and sent to an output buffer, whereas a portion other than the particular portion is not encrypted but is directly sent to the output buffer. Thereafter, the contents in the output buffer are transmitted. The particular data includes a control code of print data, upper bits of image data, predetermined discrete bits of voice data, a conversion tale for compression data, and the like.

FIG. 1

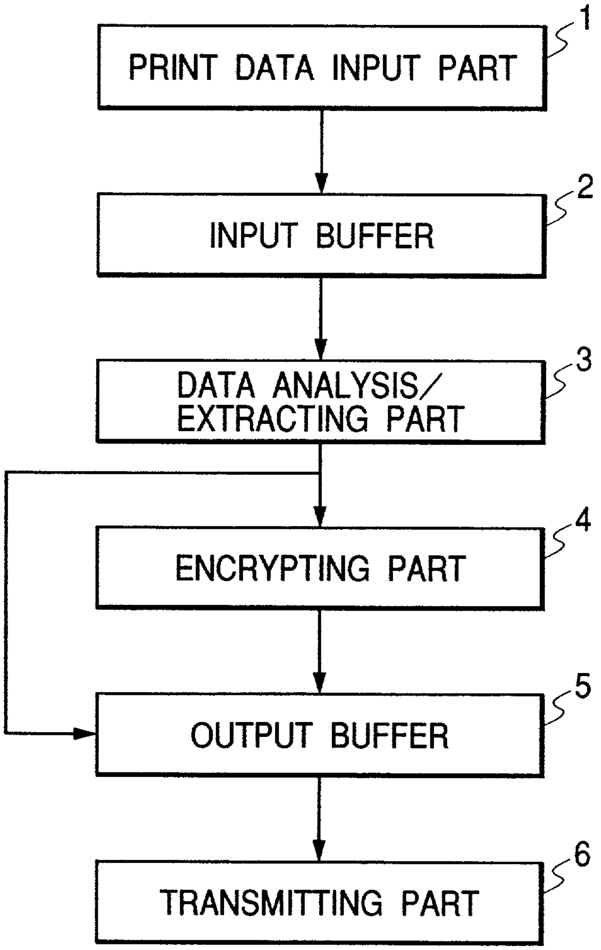

PRINT DATA INPUT PART
1
INPUT BUFFER
2
DATA ANALYSIS/ EXTRACTING PART
3
ENCRYPTING PART
4
OUTPUT BUFFER
5
TRANSMITTING PART
6

FIG. 2

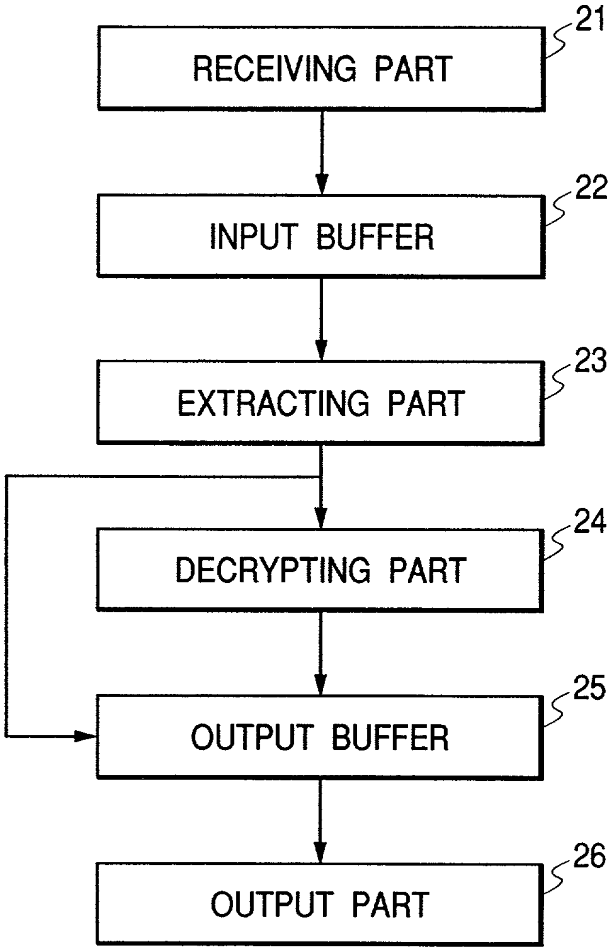

RECEIVING PART
21
INPUT BUFFER
22
EXTRACTING PART
23
DECRYPTING PART
24
OUTPUT BUFFER
25
OUTPUT PART
26

FIG. 3

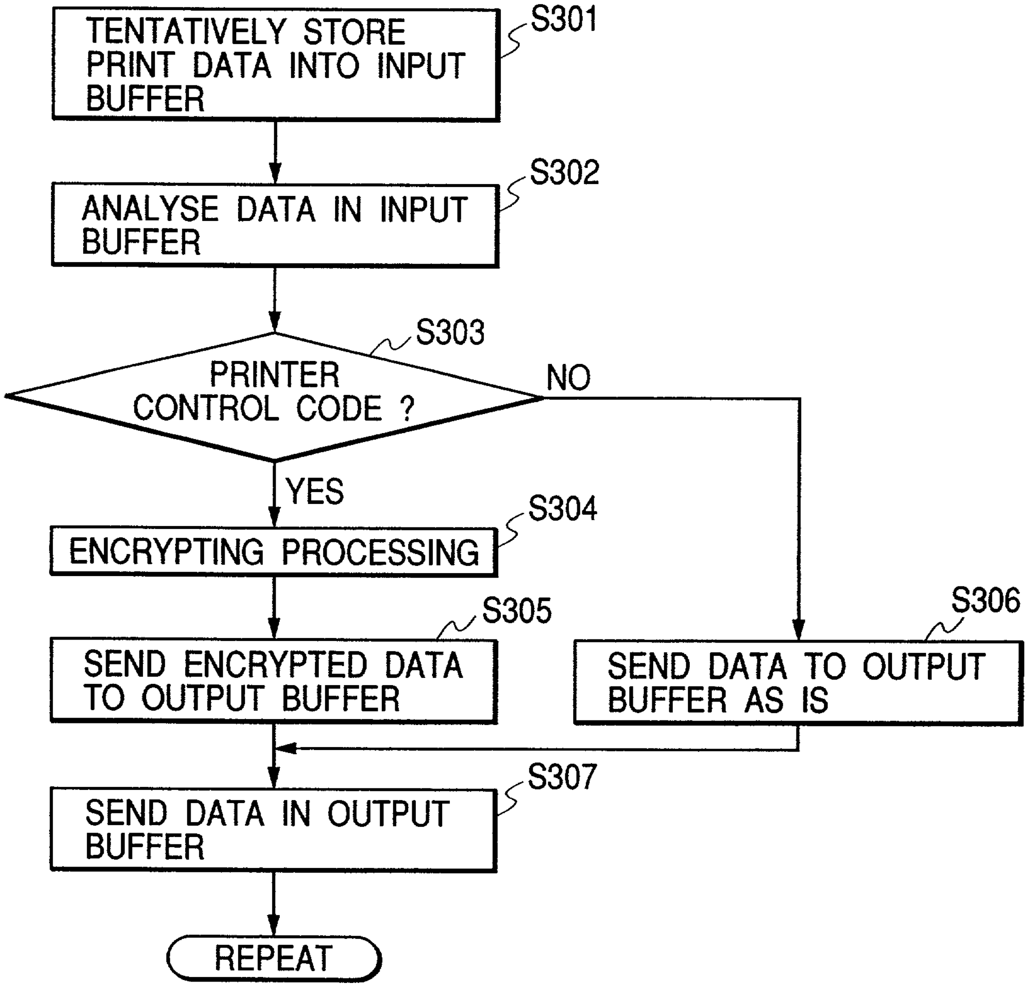

TENTATIVELY STORE PRINT DATA INTO INPUT BUFFER
S301
ANALYSE DATA IN INPUT BUFFER
S302
PRINTER CONTROL CODE ?
S303
NO
YES
ENCRYPTING PROCESSING
S304
SEND ENCRYPTED DATA TO OUTPUT BUFFER
S305
SEND DATA TO OUTPUT BUFFER AS IS
S306
SEND DATA IN OUTPUT BUFFER
S307
REPEAT

FIG. 4

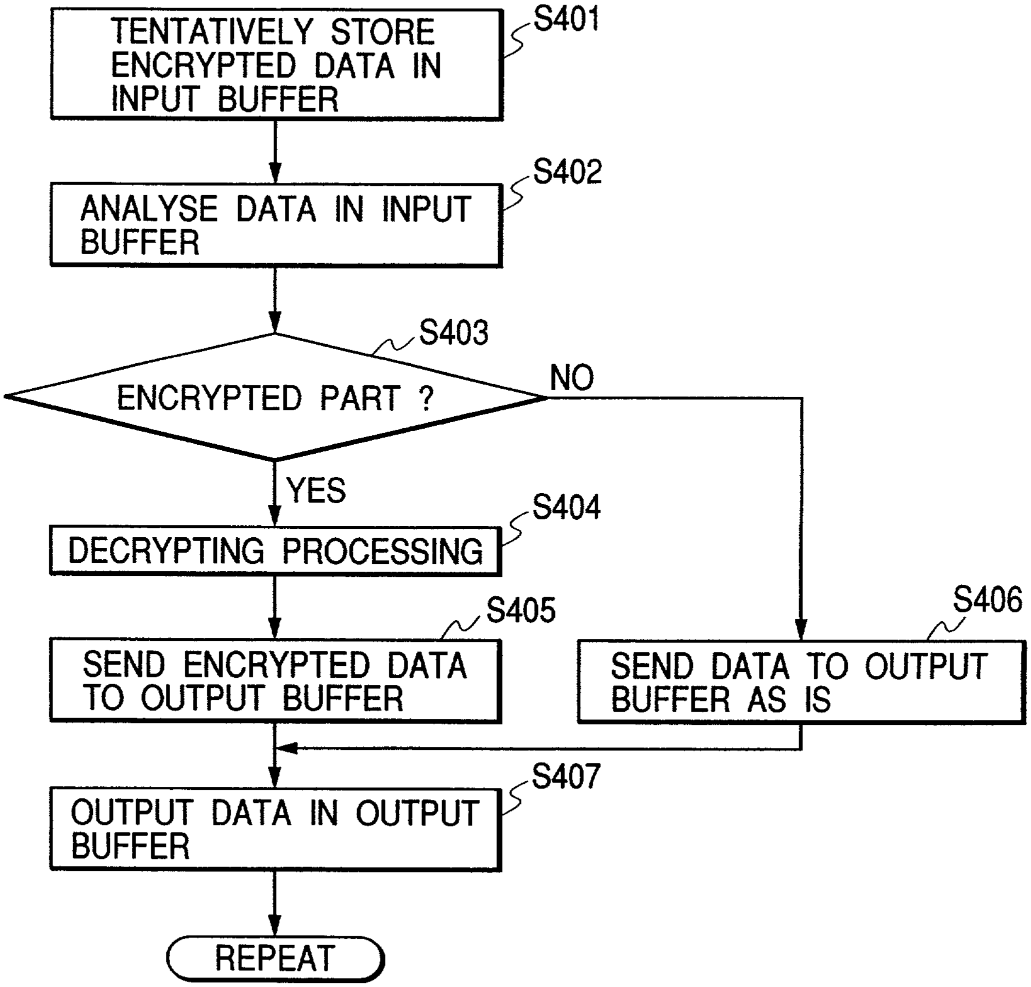

TENTATIVELY STORE ENCRYPTED DATA IN INPUT BUFFER
S401
ANALYSE DATA IN INPUT BUFFER
S402
ENCRYPTED PART ?
S403
NO
YES
DECRYPTING PROCESSING
S404
SEND ENCRYPTED DATA TO OUTPUT BUFFER
S405
SEND DATA TO OUTPUT BUFFER AS IS
S406
OUTPUT DATA IN OUTPUT BUFFER
S407
REPEAT

FIG. 5

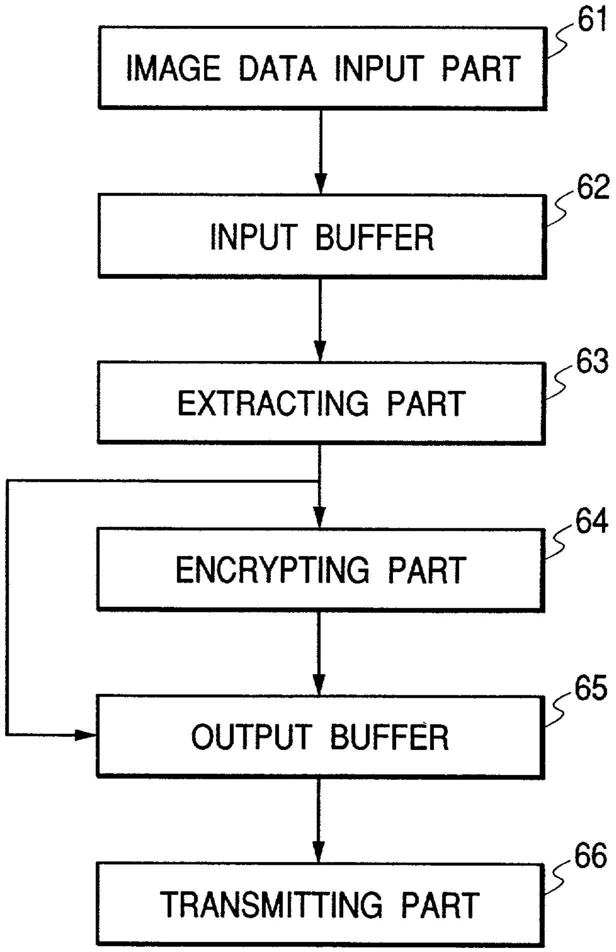


IMAGE DATA INPUT PART
61
INPUT BUFFER
62
EXTRACTING PART
63
ENCRYPTING PART
64
OUTPUT BUFFER
65
TRANSMITTING PART
66

FIG. 6

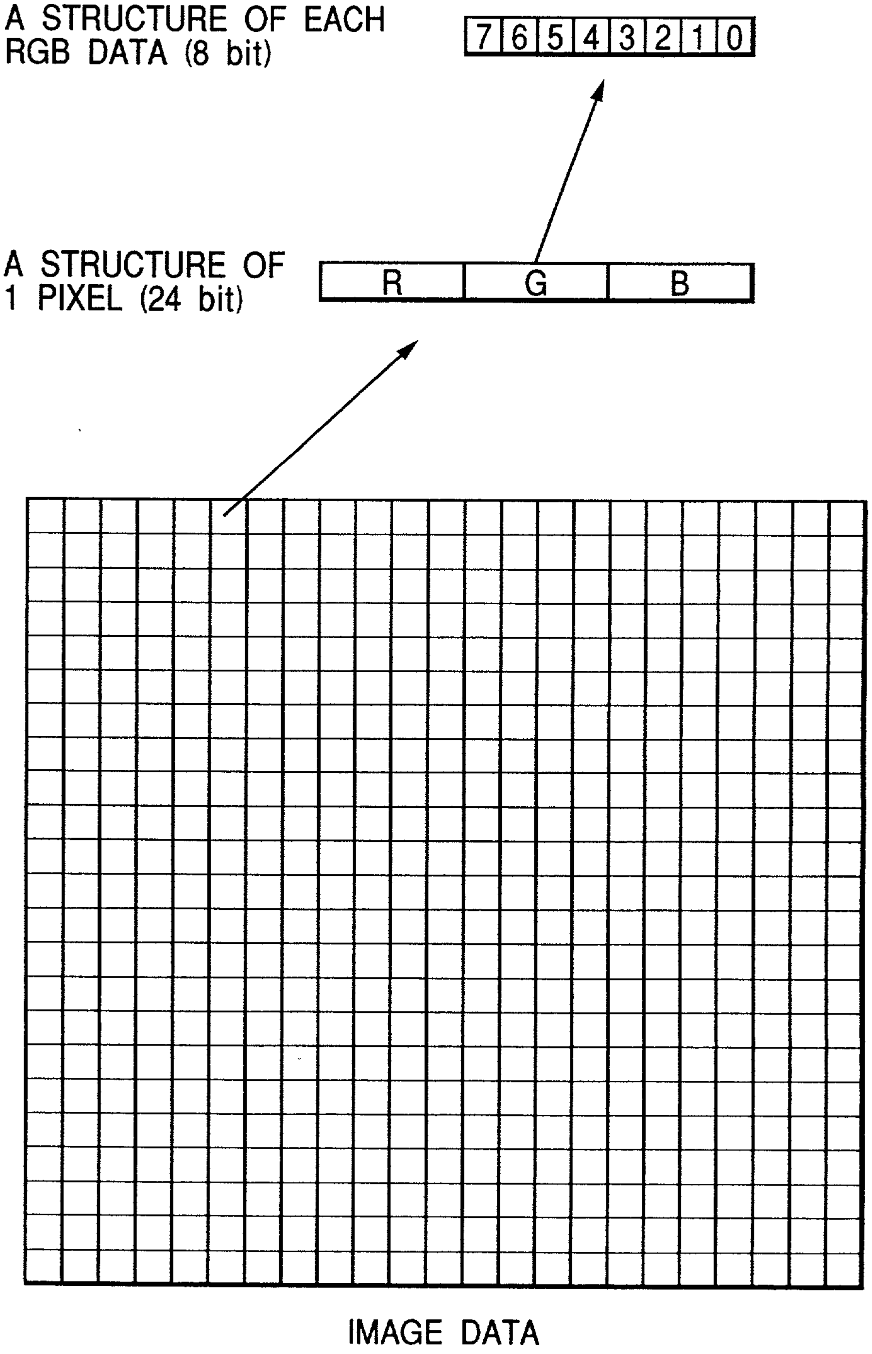

A STRUCTURE OF EACH RGB DATA (8 bit)
7
6
5
4
3
2
1
0
A STRUCTURE OF 1 PIXEL (24 bit)
R
G
B
IMAGE DATA

FIG. 7

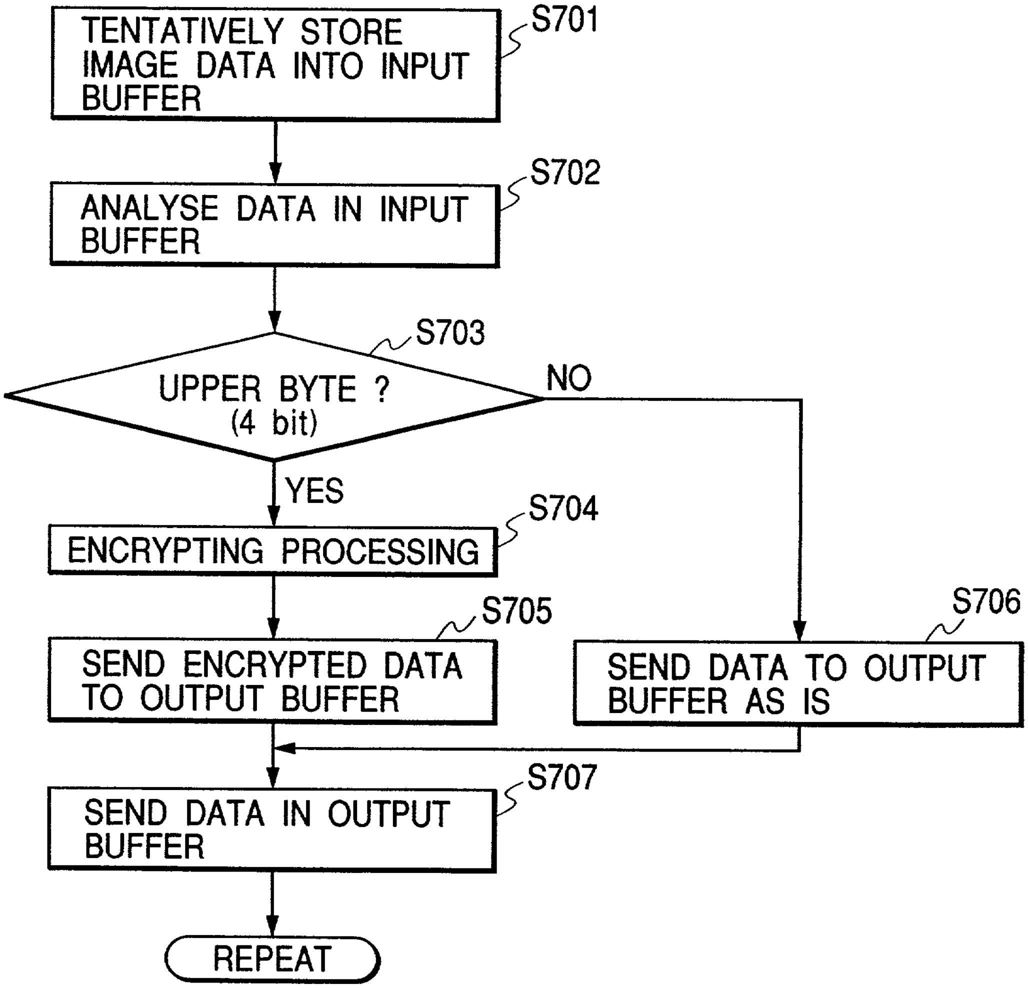

TENTATIVELY STORE IMAGE DATA INTO INPUT BUFFER
S701
ANALYSE DATA IN INPUT BUFFER
S702
UPPER BYTE ? (4 bit)
S703
NO
YES
ENCRYPTING PROCESSING
S704
SEND ENCRYPTED DATA TO OUTPUT BUFFER
S705
SEND DATA TO OUTPUT BUFFER AS IS
S706
SEND DATA IN OUTPUT BUFFER
S707
REPEAT

FIG. 8

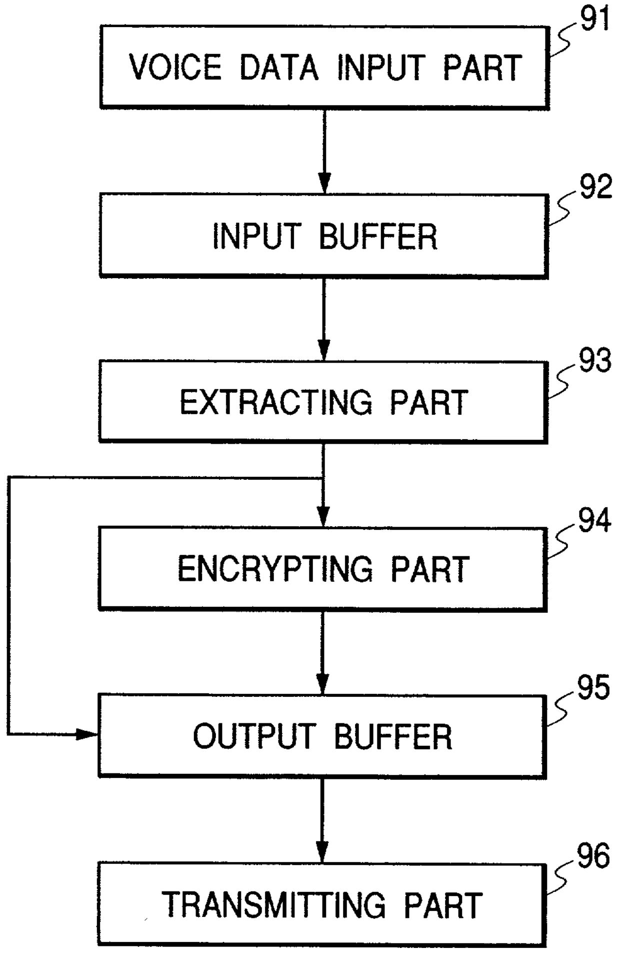

VOICE DATA INPUT PART
91
INPUT BUFFER
92
EXTRACTING PART
93
ENCRYPTING PART
94
OUTPUT BUFFER
95
TRANSMITTING PART
96

FIG. 9A

FIG. 9B

FIG. 9C

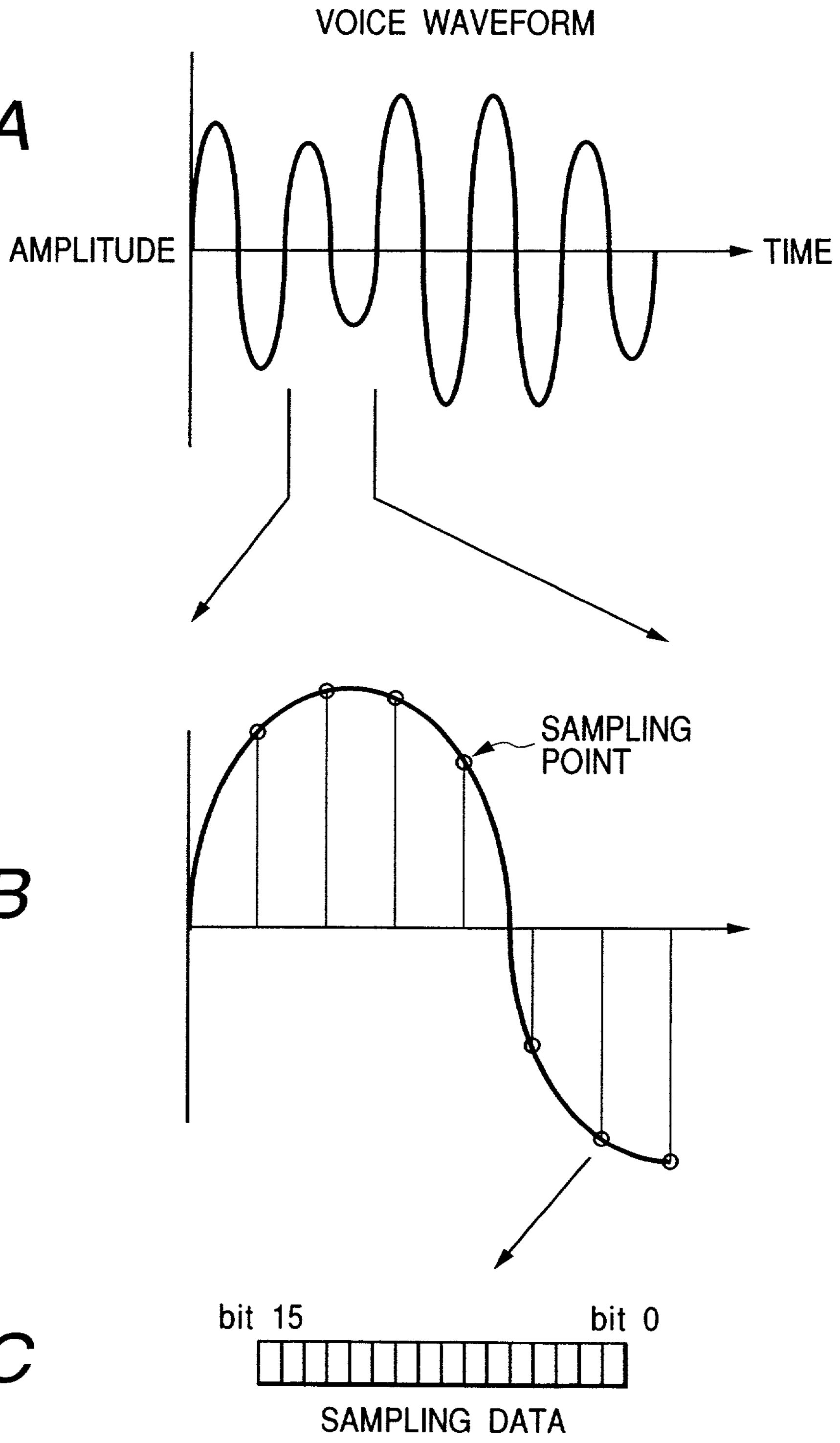


FIG. 10

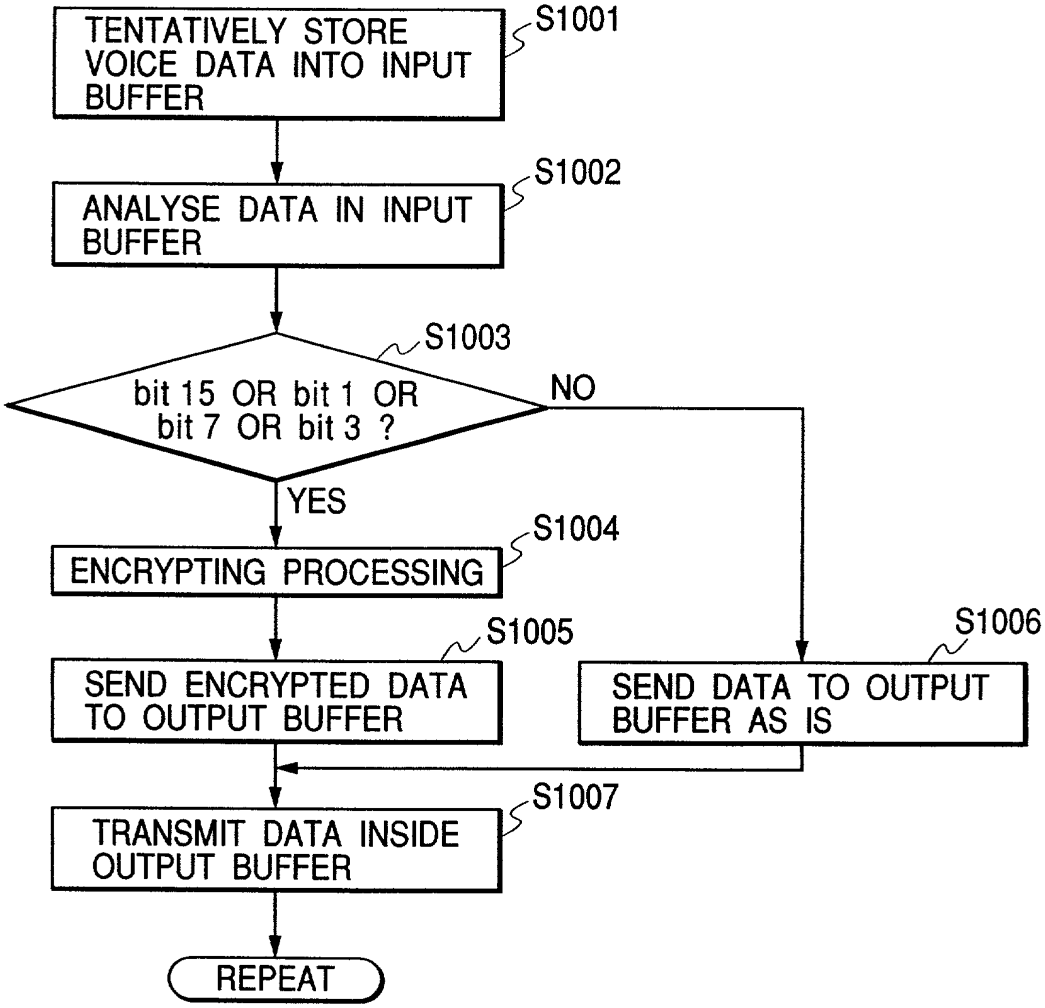

TENTATIVELY STORE VOICE DATA INTO INPUT BUFFER
S1001
ANALYSE DATA IN INPUT BUFFER
S1002
bit 15 OR bit 1 OR bit 7 OR bit 3 ?
S1003
NO
YES
ENCRYPTING PROCESSING
S1004
SEND ENCRYPTED DATA TO OUTPUT BUFFER
S1005
SEND DATA TO OUTPUT BUFFER AS IS
S1006
TRANSMIT DATA INSIDE OUTPUT BUFFER
S1007
REPEAT

FIG. 11

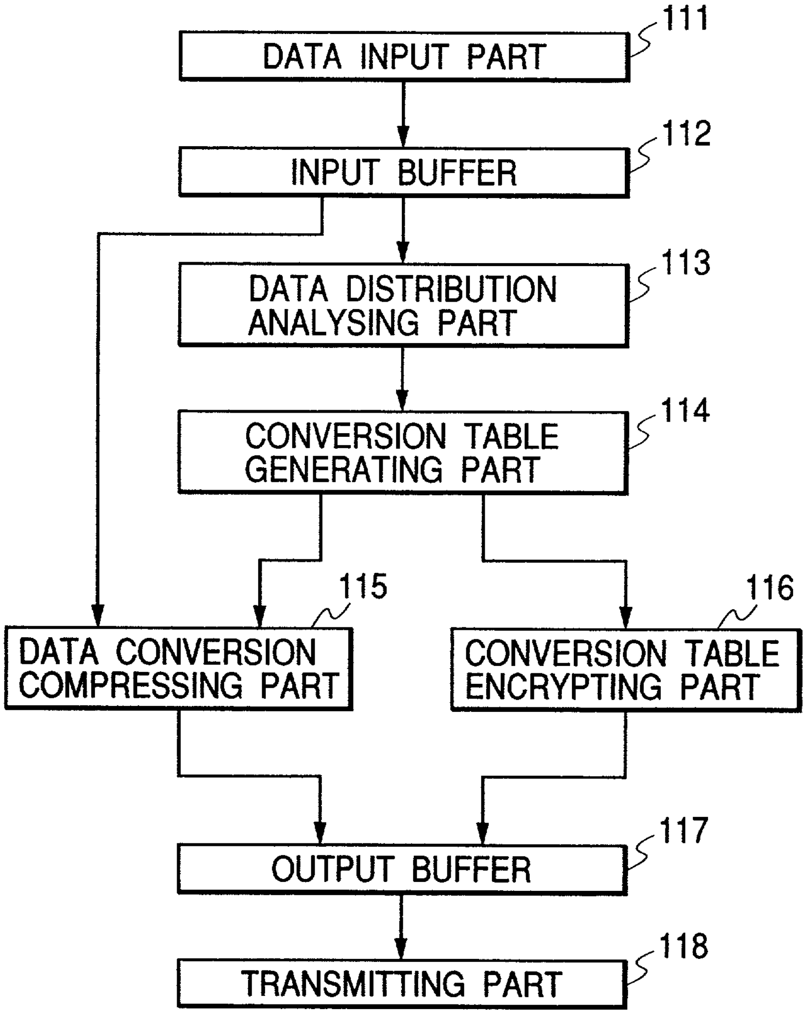
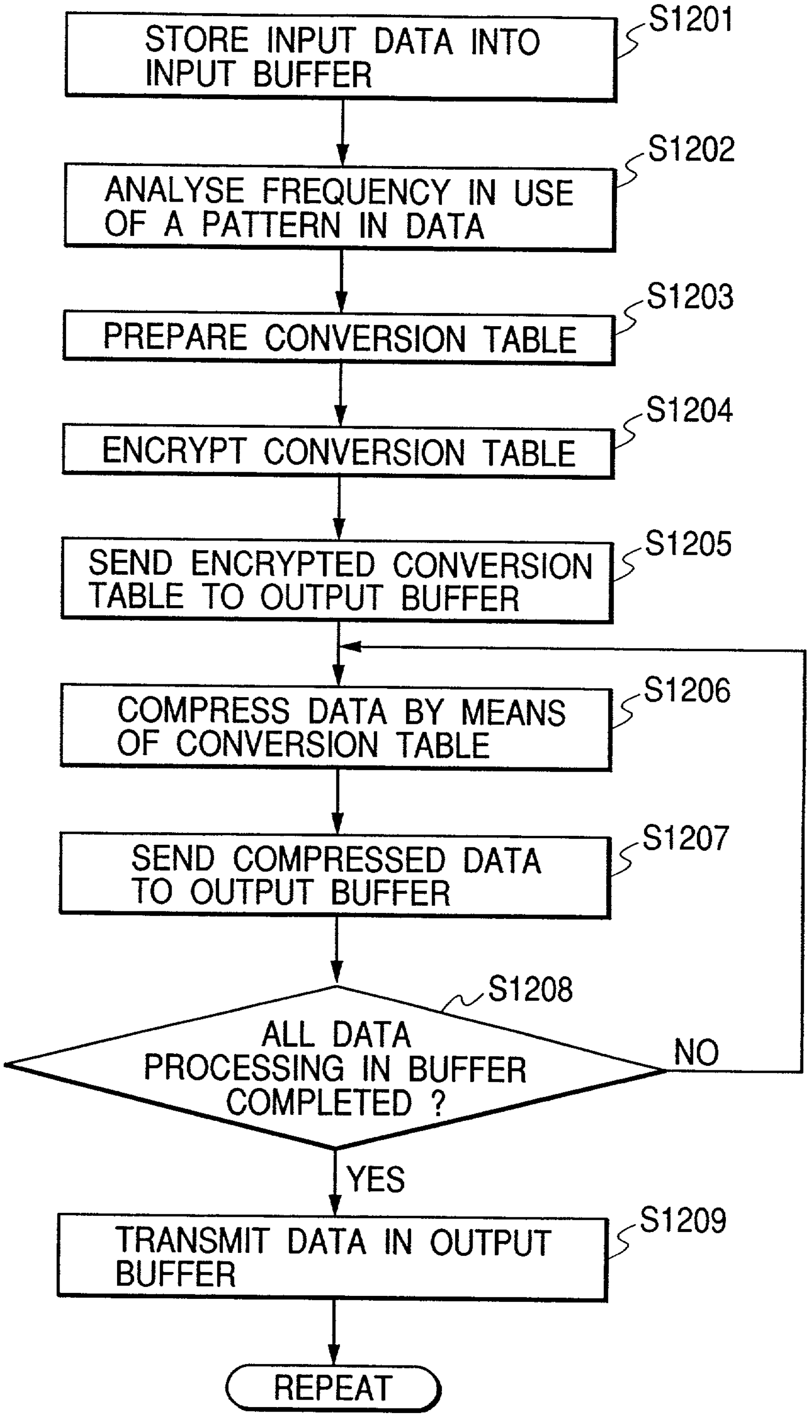

DATA INPUT PART
111
INPUT BUFFER
112
DATA DISTRIBUTION ANALYSING PART
113
CONVERSION TABLE GENERATING PART
114
DATA CONVERSION COMPRESSING PART
115
CONVERSION TABLE ENCRYPTING PART
116
OUTPUT BUFFER
117
TRANSMITTING PART
118

FIG. 12


STORE INPUT DATA INTO INPUT BUFFER
S1201
ANALYSE FREQUENCY IN USE OF A PATTERN IN DATA
S1202
PREPARE CONVERSION TABLE
S1203
ENCRYPT CONVERSION TABLE
S1204
SEND ENCRYPTED CONVERSION TABLE TO OUTPUT BUFFER
S1205
COMPRESS DATA BY MEANS OF CONVERSION TABLE
S1206
SEND COMPRESSED DATA TO OUTPUT BUFFER
S1207
ALL DATA PROCESSING IN BUFFER COMPLETED ?
S1208
NO
YES
TRANSMIT DATA IN OUTPUT BUFFER
S1209
REPEAT

COMBINED DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION
(Page 1)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name ıs listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled DATA PROCESSING APPARATUS AND METHOD FOR ENCRYPTION OR DECRYPTION OF COMMUNICATION DATA

the specification of which ☒ ıs attached hereto □ was filed on ______________ as United States Application No or PCT International Application No. ______________
and was amended on ______________ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined ın 37 CFR §1.56.

I hereby claim foreign priority benefits under 35 U.S.C. §119(a)-(d) or §365(b), of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT international application which designates at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT international application having a filing date before that of the application on which priority is claimed:

Country	Application No.	Filed (Day/Mo./Yr.)	(Yes/No) Priority Claimed
JAPAN	11-076758	19 MARCH 1999	Yes

I hereby claim the benefit under 35 U.S C § 120 of any United States application(s), or § 365(c) of any PCT international application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 C.F R § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

Application No.	Filed (Day/Mo./Yr.)	Status (Patented, Pendıng, Abandoned)

I hereby appoint the practitioners associated with the firm and Customer Number provided below to prosecute this application and to transact all business ın the Patent and Trademark Office connected therewith, and direct that all correspondence be addressed to the address associated with that Customer Number:

FITZPATRICK, CELLA, HARPER & SCINTO
Customer Number: 05514

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on ınformation and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole or First Inventor Masahiko YAMAGUCHI

Inventor's signature ______________

Date ______________ Citizen/Subject of Japan

Residence 5-12-401, Hirakawa-cho, Kanagawa-ku, Yokohama-shi,
Kanagawa-ken, Japan

Post Office Address c/o CANON KABUSHIKI KAISHA, 30-2, Shimomaruko 3-chome, Ohta-ku,
Tokyo, Japan

BLK\cmv